Information Security Advisory Council
Goals and Objectives – 2015 Biennium

Mission

The mission of the State of Montana's Information Security Advisory Council (ISAC) is to ensure that Montana's information systems are safe, secure, and resilient.

Three key concepts provide the foundation of this vision:

- Governance
- Posture
- Response

In turn, these key concepts will drive broad areas of activity that will define the ISAC objectives for the next two years. These goals and objectives define a framework to describe what it means to identify, prevent, protect, respond and recover, as well as incorporate security into Montana's information systems to ensure resilience.

Goals

- Advance Montana's overall security **Governance** by adopting a framework of standards and processes.
- Advance Montana's overall security **Posture** though proactive risk management, cyber workforce development, and industry best practices for cybersecurity.
- Advance Montana's over all security **Response** to the ever-changing cybersecurity landscape.

Objectives

- **Governance**
    - Establish through Executive Order an Information Security Advisory Council (ISAC) that includes state, local, National Guard, and private sector representation.
    - Implement an Enterprise Security Program in conjunction with the ISAC to ensure effective implementation of cybersecurity in all agencies of state government.
    - Develop an interagency information security strategy with initiatives, priorities, policies, standards, and roles and responsibilities to enhance the state cybersecurity posture.
    - Update State of Montana cybersecurity policies to align with the NIST Cybersecurity Framework.

- Begin the enterprise program by addressing gaps focusing on state government and expanding to the private sector over time through the use of the ISAC.
- Develop standard accountability processes for Department heads to ensure cybersecurity.
- Create a strategy to promote cybersecurity situational awareness for all users.
- Foster better communication in cybersecurity between federal, state, local, and tribal governments.
  - Formalize information sharing protocol and document standing information needs between HSA, DOA/SITSD/CISO, AND DOJ/DIC/MATIC.
- Understand the value of the University System's security needs
  - Document the University System perspective of their cybersecurity preparedness and the threats that they face, help develop a strategy of best practices, and assist with how to best promote cybersecurity.
- Encourage development of a trained and educated cybersecurity workforce in Montana through the University System with private sector input
  - Include an apprenticeship or internship program to develop hands-on cybersecurity skills.
- Understand the value of the Local Government security needs.
  - Document the Local Government perspective of their cybersecurity preparedness and the threats that they face, help develop a strategy of best practices, and assist with how to best promote cybersecurity.
- Understand the value of the Montana Local Business security needs.
  - Document the Local Business perspective of their cybersecurity preparedness and the threats that they face, help develop a strategy of best practices, and assist with how to best promote cybersecurity.
- Recommend new legislation or updates to existing laws such as reporting requirements to government and citizens as appropriate.
  - Create recommendations to update current state statutes, both administrative statutes for state government needs and criminal statutes to address the present-day cybersecurity environment.

➢ **Posture**

- Begin to assess security posture and readiness of each Department in state government.
- Develop strategy for better patch management
- Develop limited user rights strategy for state information systems.
- Identify legacy systems which exist on the State of Montana network and create a plan for securing or removing those systems.

- Develop a campaign to deliver the message of cybersecurity in a positive and informational manner that engages the listener and encourages them to integrate cybersecurity into his daily activities.
- Support a statewide cybersecurity training program to serve technical and managerial needs.
- Collaborate with private industry to understand the cybersecurity posture of critical infrastructure.
- Establish a communications procedure for receiving input from and sharing information with the public, state agencies, and local governments.
- Develop a Governor's cybersecurity dashboard
- Provide a yearly information security assessment to the Governor showing program successes and shortcomings with a plan to address shortcomings.
- Conduct internal evaluations of the statewide cybersecurity program.
- Explore training of DOA/DOJ/National Guard staff to defend against cyber-attacks through the use of the State of Washington National Guard cyber unit.
- Evaluate the State of Washington's best practices of the cyber unit of the National Guard and apply its practices in Montana where applicable.
- Recommend appropriate cost-effective safeguards to reduce, eliminate, or recover from identified threats to data.
- Develop a plan to increase the education of Montana's law enforcement group regarding cybersecurity.
- Advise on security requirements in the specifications for solicitation of state contracts for procuring information technology resources.
- Develop and implement a state Risk Management services program.

- **Response**
  - Recommend resources (funding, people, etc.) and possible methods to obtain cybersecurity teams, in order to enhance the State information security posture.
  - Move forward with state preparedness and migrate toward evaluation of the role with private sector as time and resources allow.
  - Assess the feasibility of Security Assistance Teams (SAT). Teams may be comprised of security representatives from state agencies to help with risk assessments, make recommendations, write documents, and conduct training to help agencies be more secure based on ISAC direction and industry best practices.
  - Research and recommend criminal investigative response in coordination with HSA, DOA, DOJ, and FBI.
  - Explore additional resources in DOJ/DCI for Network Cyber Investigations.
  - Improve the State of Montana's investigative expertise in the cybersecurity area.
  - Provide technical and managerial assistance relating to cybersecurity.